UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,933	10/01/2003	Richard H. Boivie	YOR920030398US1 (8728-647	9603

46069 7590 01/31/2012

F. CHAU & ASSOCIATES, LLC
Frank Chau
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
01/31/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mail@chauiplaw.com
garramone@chauiplaw.com
uspto1@chauiplaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/677,933	BOIVIE ET AL.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *11,13,14,16-19 and 22-29* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *11, 13-14,16-19 and 22-29* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 11/28/2007.

Response to Arguments

Applicant's arguments have been fully considered but they are not persuasive. Sudia in view of Abbondanzio is not a improper combination. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

Applicant's arguments with respect to Sudia in view of Abbondanzio have been fully considered but they are not persuasive. The combination teaches how to execute signed authorized code that embodies a boot process. Sudia paragraph 0249 teaches i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto … upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device …verify the third party's signature on the new code routines against the manufacturer's upgrade certificate.

Abbondanzio teaches that authorized code is authorized boot code including instructions for performing a boot process for a computer device comprising the processor (see paragraph 0036). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

Applicant's arguments that Abbondanzio the boot code is executed on a network off the system that is booted have been fully considered but they are not persuasive. Figure 6 steps 607 – 609 teach the encrypted boot code image is transmitted to the appropriate server where it is authenticated and run. This is also taught in paragraphs 0058-0060 i.e. "If the received boot code image is authenticated, then server blade 110 may boot the received boot code image in step 609. That is, if the authentication parameter(s), e.g., public key, received by server blade 110 in step 605 decrypt the received encrypted boot code image, then server blade 110 may boot the received boot code image in step 609".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11, 14, 16, 18 and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) in view of Mattison (5778070) in view of Abbondanzio et al (2003/0188176).

With respect to calms 11 and 22, a method for ensuring that a processor will execute only authorized code, said method comprising: reading a certificate including a first public key into a protected memory (see paragraph 0249 i.e. the manufacturer could sign a firmware upgrade certificate containing a public key of the third party firmware provider and issue it to that third party… upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device); validating said certificate with a second public key permanently stored on said processor (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture); reading a signed authorized code into said protected memory (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate

from the manufacturer thereto … upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); reading by said processor a digital signature used to sign said signed authorized boot code; verifying said decrypted digital signature in accordance with said first public key (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate); and executing by the processor said signed authorized code having a verified digital signature by branching to a copy of said authorized code in said protected memory, wherein said digital signature of said signed authorized boot code is previously verified and executing further comprises performing inline decryption of the copy of said authorized code in said protected memory (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

Sudia does not teach decrypting the digital signature to generate a decrypted digital signature and that authorized code is authorized boot code

including instructions for performing a boot process for a computer device comprising the processor.

Mattison teaches decrypting the digital signature to generate a decrypted digital signature (see column 3 lines 1-50). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have decrypted the digital signature to get the hash value that can be compared to a generated hash value to verify that the data that the digital signature id for has not been tampered with (see Mattison column 3 lines 1-50. Therefore one would have been motivated to have decrypted the digital signature.

Abbondanzio teaches that authorized code is authorized boot code including instructions for performing a boot process for a computer device comprising the processor (see paragraph 0036). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code. Therefore one would have been motivated to have Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code.

With respect to claim 13, wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 14 and 25, wherein said protected memory is physically protected (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 16 and 26, wherein the integrity of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 18, wherein the privacy of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claim 23, a computing device for securely executing authorized code, said computing device comprising: a protected memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer) for storing a signed authorized boot code, which contains an original digital signature (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto … upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital

signed data is a type of cryptographically protected data); and a processor comprising inline cryptography and integrity hardware for excuting said signed authorized boot code said processor in signal communication with said protected memory said processor reading and decrypting said signed authorized boot code from the protected memory and executing said signed authorized boot code from the protected memory for booting the computing device after verifying that said digital signature contained in said signed authorized boot code is valid as decrypted in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor, and branching to said signed authorized boot code in said protected memory to begin the execution (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture).

With respect to claim 24, wherein the integrity of the contents of said protected memory is protected by encryption (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claim 29, a first summing block summing said read copy of said signed authorized boot code from the protected memory with a whitening value; a decryption block decrypting an output of said first summing block; a second summing block summing an output of said decryption block with said whitening value to generate plaintext data corresponding to said copy of said signed authorized boot code from said protected memory; and a function block validating said plaintext data for execution (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture).

Claims 17, 19, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) view of Abbondanzio et al (2003/0188176) in view of Morgan et al (U.S. Patent # 6,185,685).

With respect to claims 17 and 27, Sudia and Abbondanzio do not teach wherein the integrity of said authorized code is protected with symmetric key encryption. Morgan teaches wherein the integrity of said authorized code is

protected with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31). Morgan teaches using a symmetric key to encrypt and decrypt the encrypted public key (see Morgan column 8 line 60 - column 9 lines 31). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a symmetric key to encrypt and decrypt the encrypted public key to increase the security to the encryption algorithm (see Morgan column 2 lines 32-65). Therefore one would be motivated to have encrypted the authorized code with a symmetric key before storing it in the protected memory and decrypted the authorized code with the symmetric key for execution of the authorized code.

With respect to claims 19 and 28, wherein the privacy of said authorized code is protected at run time with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The

fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432